IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MATTHEW COUNTS and KAITIA CHARITABLE, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

RICHMOND UNIVERSITY MEDICAL CENTER,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Matthew Counts and Kaitia Charitable (collectively "Plaintiffs") brings this Class Action Complaint ("Complaint"), on behalf of themselves and all others similarly situated, against Defendant Richmond University Medical Center ("RUMC" or "Defendant"), alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

I. INTRODUCTION

1. Entities that gather and retain sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of consumers' PII

or PHI to unauthorized people, especially hackers with nefarious intentions—will cause harm to such individuals.

2. Plaintiffs bring this class action lawsuit to address Defendant's unlawful and widespread unauthorized practice of disclosing Plaintiffs' and Class Members' PII and PHI (collectively referred to as Private Information) to third parties. As explained in more detail below, Defendant warrants that the services it offers on its website are safe and secure. For example, it represents: "We, at Richmond University Medical Center (RUMC) are committed to protecting the privacy of information we gather about you while providing health-related services."[1]

3. Defendant further assures consumers that "we are required by law to protect the privacy of health information that may reveal your identity, and to provide you with a copy of this notice, which describes the health information privacy practices of RUMC, its medical staff, and affiliated health care providers that jointly provide health care services with RUMC."[2]

4. Contrary to its assurances, Defendant did not maintain adequate systems and procedures to ensure the security of the highly sensitive PII and PHI consumers entrusted to it. As a result, Defendant was the target of a data breach ("Data Breach") in which Plaintiffs' and Class members' Private Information was exposed to hackers and/or cybercriminals. Defendant published the following notice on its website: "We discovered

[1] Richmond University Notice of Privacy Practices (https://www.rumcsi.org/careers/our-mission/notice-of-privacy-policy) (last accessed December 30, 2024).
[2] *Id.*

unauthorized access to our network that resulted in unauthorized access to, or acquisition of, certain files by an unauthorized actor."[3]

5. In the website notice, Defendant claimed that it learned of the Data Breach on May 6, 2023. Upon information and belief, most consumers did not know about the data breach until receiving a letter notice from Defendant more than nineteen months after Defendant had learned of the Data Breach ("Notice Letter"), on December 19, 2024.

6. The PII and PHI compromised in the Data Breach included information concerning current and former employees and patients, including Plaintiffs. This Private Information included but is not limited to names, addresses, dates of birth, face sheets, imaging reports, Social Security numbers, government identification information/driver's license numbers, health insurance information, and medical information.[4]

7. The harm resulting from a breach of private data manifests in several ways, including identity theft, financial fraud, and the filing of false medical claims. The exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and

[3] Richmond University Medical Center Notifies Potentially Affected Individuals of Information Security Incident" (https://www.rumcsi.org/wp-content/uploads/2024/12/Richmond-University-Medical-Center-Notifies-Potentially-Affected-Individuals-of-Information-Security-Incident32482687.1.pdf (last accessed December 30, 2024).

[4] *Id.* (last accessed December 30, 2024).

money to closely monitor their credit, financial accounts, health records, and email accounts, as well as other prophylactic measures.

8. As discussed in more detail below, Defendant breached its duty to protect the sensitive entrusted to it, failed to abide by its own Privacy Policy, and failed to provide sufficiently prompt notice after learning of the Data Breach. As such, Plaintiffs bring this Class action on behalf of himself and the other consumers whose Private Information was accessed and exposed to unauthorized third parties during the Data Breach (the "Class").

9. As a direct and proximate result of Defendant's inadequate data security, and breach of its duty to handle Private Information with reasonable care, Plaintiffs' Private Information has been accessed by hackers and exposed to an untold number of unauthorized individuals.

10. Plaintiffs are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of his health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

11. Plaintiffs, on behalf of themselves and others similarly situated, bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, breach of an implied contract, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

12. To recover from Defendant for his sustained, ongoing, and future harms, Plaintiffs seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of Private Information possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

II. PARTIES

13. Plaintiff Matthew Counts is an adult who at all relevant times was a citizen of New York and currently resides at 869 Forrest Avenue, Staten Island, New York. Count's Private Information was stored and handled by Defendant on its systems. During or around December 19, 2024, Counts was notified by Defendant via letter dated December 19, 2024 of the Data Breach occurring on or around May 6, 2023 and the impact to his Private Information.

14. Plaintiff Kaitia Charitable is an adult who at all relevant times was a citizen of New York and currently resides at 62 Sable Loop, Staten Island, New York. Charitable's Private Information was stored and handled by Defendant on its systems. During or around December 19, 2024, Moore was notified by Defendant via letter dated December 19, 2024 of the Data Breach occurring on or around May 6, 2023 and the impact to her Private Information.

15. As a result of Defendant's conduct, Plaintiffs suffered actual damages including, without limitation, time related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, misappropriation of health insurance benefits, and exposure and misuse of their private health information. Plaintiffs and Class members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial and health insurance accounts, and monitor for fraud or identify theft – particularly since the compromised information may include Social Security numbers and private insurance information.

16. Defendant Richmond University Medical Center. is a New York domestic not for profit corporation with its principal place of business at 355 Bard Avenue, Staten Island, New York.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's states of citizenship.

18. This Court has personal jurisdiction over Defendant in this case because Defendant is headquartered and has its principal place of business in this District. Defendant also conducts substantial business and has minimum contacts with the State of New York.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant

is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant and the Services it Provides

20. Defendant is a full service, nonprofit hospital and healthcare provider serving Staten Island, New York, and the surrounding communities.

21. Defendant offers a broad spectrum of services, including emergency care, behavioral health, surgical services, maternity care, pediatrics, and specialized programs such as cardiology, oncology, and neurology. A large amount of data held by Defendant is of a highly sensitive and private nature.

22. This highly sensitive and private information is collected while Defendant administers its services, which includes, *inter alia*: social security numbers; first and last names; dates of birth; zip codes; states of residence; full mailing and email addresses; employers with contact information; primary and secondary insurance policy holders' names, addresses, dates birth, and social security numbers; demographic information; drivers licenses or state or federal identification; medical conditions and histories; insurance information and coverage; and banking and/or credit card information. Critically, Defendant creates and stores comprehensive medical records and other protected health information for its patients.

23. To receive services from Defendant, Plaintiffs are required to entrust their highly sensitive Private Information to Defendant. Plaintiffs entrusted this information to Defendant with reasonable expectation and mutual understanding that Defendant would

comply with its obligations to keep such information confidential and secure from unauthorized access.

24. Further, upon information and belief, RUMC's HIPAA Notice of Privacy Practices is provided to every patient both prior to receiving treatment and upon request.[5] This Notice demonstrates that RUMC knows its patients' Private Information is highly sensitive and is necessarily protected by law.

25. By obtaining, collecting, and storing Plaintiffs' Private Information, Defendant assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiffs' Private Information from unauthorized disclosure.

26. And, upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class members.

B. Data Breach

27. At all relevant times, Defendant knew it was storing sensitive Private Information and that, as a result, its systems would be an attractive target for cybercriminals.

28. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

[5] RUMC Notice of Privacy Practices (https://www.rumcsi.org/careers/our-mission/notice-of-privacy-practices/) (Last accessed December 30, 2024).

29. These risks are not theoretical. The health industry has become a prime target for threat actors.

30. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

31. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[6]

32. The United States Office for Civil Rights established, as part of the department of Health and Human Services ("HHS"), a "Breach Portal" to address the widespread issue of data breach.

33. Upon information and belief, Defendant was aware of the Data Breach as early as May 6, 2023. It therefore waited over nineteen months before reporting the Data Breach to the HHS, and before sending Notice to affected patients.

34. RUMC's Notice letter, sent to Plaintiffs and Class members on or about December 19, 2024, listed time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing for a small subset of Class Members to affirmatively sign up for a call center to contact with questions, Defendant

[6] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 17, 2023).

offered no other substantive steps to help victims like Plaintiffs and the Class to protect themselves.

35. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's consumers especially vulnerable to identity theft, tax fraud, medical fraud, insurance fraud, credit and bank fraud, and more.

36. PII and PHI are valuable property rights.[7] The value of Private Information as a commodity is measurable.[8] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[9] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[10] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[7] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[8] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle./824192.

[9] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[10] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

37. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, PHI and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

38. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[11]

39. Even if stolen Private Information does not include financial or payment card account information, it does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained Private Information about the individual, such as name, address, email

[11] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 17, 2023).

address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

40. Further, according to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 713 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR—an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[12]

41. Health organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The Private Information stored is highly detailed, and that information can be easily monetized."[13]

42. Patient records are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The fullz are then sold on the dark web to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[14]

---

[12] Steve Alder, "Editorial: Why Do Criminals Target Medical Records", The HIPAA Journal (https://www.hipaajournal.com/why-do-criminals-target-medical-records/) (Nov. 2, 2023).
[13] *Id.*
[14] *Id.*

43. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites." [15]

44. Health organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The Private Information stored is highly detailed, and that information can be easily monetized."[16]

45. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

46. Based on the value of consumers' Private Information to cybercriminals and the growing rate of data breaches (not to mention the obligations created by HIPAA and the Federal Trade Commission Act), Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Defendant Breached its Duty to Protect Plaintiff's and Class Members' Private Information

[15] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

[16] *Id.*

47. During December 2024—over nineteen months after learning of the Data Breach—Defendant announced on its website that it experienced a security incident disrupting access to its systems.

48. As noted above, the Private Information compromised in the Data Breach includes consumers' names, dates of birth, Social Security Numbers, full mailing and email addresses, and comprehensive medical and insurance information.

49. Like Plaintiffs, other potential Class members received mail notice informing them that their Private Information was exposed in the Data Breach.

50. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures necessary to protect its consumers' Private Information.

D. The FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices

51. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

52. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

53. The FTC provides cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[18]

54. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting

[17] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[18] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n,(https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf).

[19] *Id.*

from these actions further clarify the measures businesses must take to meet their data security obligations.

56. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

E. **Defendant's Conduct Violates HIPAA**

57. HIPAA requires covered entities such as Defendant to protect against reasonable anticipated threats to the security of PHI.

58. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI, including physical, technical, and administrative components.

59. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the HHS create rules to streamline the standards for handling Private Information like that compromised in the Data Breach. The HHS subsequently promulgated regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

60. A Data Breach such as the one affecting Defendant is considered a breach under the HIPAA rules because there was access of PHI violative of the HIPAA Privacy

Rule. A breach under the HIPPA Rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security of privacy of the PHI." *See* 45 C.F.R. § 164.40.

61. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

F. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

62. Cyberattacks and data breaches targeting companies like Defendant are especially problematic because they can negatively impact on the daily lives of individuals affected by the attack.

63. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

64. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial

[20] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

65. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

66. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[21]

67. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and

[21] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

68. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

69. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[22]

70. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or

[22] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets." (citations omitted)).

undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

71. As discussed above, Private Information is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

72. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It is hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [23]

73. For instance, with a stolen Social Security number, which is only one subset of Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[24]

74. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[25] Such fraud

---

[23] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).

[24] *Id.*

[25] *Id.*

may go undetected until debt collection calls commence months, or even years later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[26] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

75. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

76. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Genworth is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal,

[26] *Id.* at 4.

[27] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

77. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[28] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[29]

78. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to Private Information, they *will use it.*[30]

79. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. As with income tax returns, an individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

---

[28] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[29] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[30] *Id.*

80. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[31]

81. Cybercriminals can post stolen Private Information on the cyber black-market for years following a data breach, thereby making such information publicly available.

82. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it happened. [32] This gives thieves ample time to seek multiple treatments under the victim's name.

83. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[33]

84. It is within this context that Plaintiffs must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

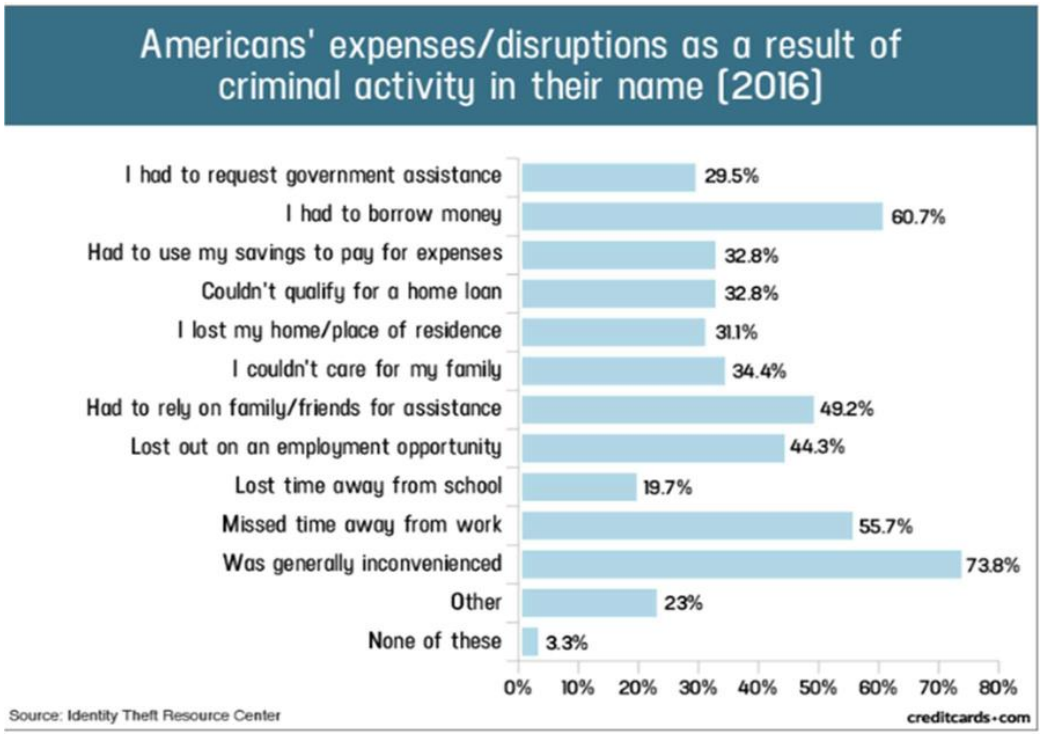
85. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.

---

[31] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[32] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Apr. 17, 2023).

[33] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.



86. Victims of the Data Breach, like Plaintiffs, must spend many hours and large sums of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[34]

87. As a direct and proximate result of the Data Breach, Plaintiffs have had their Private Information exposed, has suffered harm and has been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare

[34] *Id.*

providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

88. Moreover, Plaintiffs and Class members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' Private Information.

89. Plaintiffs and Class members also have an interest in ensuring that their personal information that was provided to Defendant is removed from Defendant's unencrypted files.

90. Because of the value of its collected and stored data, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

G. Plaintiffs Suffered Damages

91. Defendant received Plaintiffs' and Class members' Private Information in connection with providing certain financial services to them. In requesting and maintaining Plaintiff's Private Information for business purposes, Defendant expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs and Class members' Private Information. Defendant did not, however, take proper care of Plaintiffs'

and Class members' Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

92. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class members significant injuries and harm in several ways. Plaintiffs and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiffs and Class members have taken or will be forced to take these measures to mitigate their potential damages as a result of the Data Breach.

93. Once Private Information is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

94. Further, the value of Plaintiffs and Class members' Private Information has been diminished by its exposure by the Data Breach. Plaintiffs and Class members did not receive the full benefit of their bargain when paying for medical services, and instead received services that were of a diminished value to those described in their agreements with Defendant for the benefit and protection of Plaintiffs and their respective Private

Information. Plaintiffs and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

95. Plaintiffs and Class members would not have obtained services from Defendant or paid the amount they did to receive such services, had they known that Defendant would negligently fail to protect their Private Information. Indeed, Plaintiffs and Class members paid for services with the expectation that Defendant would keep their Private Information secure and inaccessible from unauthorized parties. Plaintiffs and Class members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

96. As a result of Defendant's failures, Plaintiffs and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or other misuse of their Private Information.

97. Further, because Defendant delayed posting a notice of the Data Breach on its website for over nineteen months, and delayed sending mail notice of the same to Plaintiffs and Class members for four months, Plaintiffs and Class members were unable to take affirmative steps during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

98. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only

9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[35]

99. Plaintiffs are also at a continued risk because their information remains in Defendant's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its consumers' Private Information.

100. In addition, Plaintiffs and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial and/or medical fraud, and the unauthorized exposure of their private information to strangers.

V. CLASS ALLEGATIONS

101. Plaintiffs bring all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons in the United States who had their Private Information submitted to Defendant or Defendant's affiliates and/or whose Private Information was compromised as a result of the data breach(es) by Defendant beginning in May 2023, including all who received a Notice of the Data Breach (the "Class").

102. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal

[35] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Apr. 17, 2023).

representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

103. This proposed Class definition is based on the information available to Plaintiffs currently. Plaintiffs may modify the Class definition in an amended pleading or when they move for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

104. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiffs are informed and believe, and thereon allege, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

105. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Defendant failed to timely notify Plaintiffs of the Data Breach;

b. Whether Defendant had a duty to protect the Private Information of Plaintiffs and Class members;

c. Whether Defendant was negligent in collecting and storing Plaintiffs and Class members' Private Information, and breached its duties thereby;

d. Whether computer hackers and/or cybercriminals obtained Plaintiffs' and the Class Members' Private Information;

e. Whether Plaintiffs' and the Class Members' Private Information has been posted on the dark web;

f. Whether Defendant breached its fiduciary duty to Plaintiffs and the Class;

g. Whether Defendant breached its duty of confidence to Plaintiffs and the Class;

h. Whether Defendant violated its own Privacy Practices;

i. Whether Defendant entered a contract implied in fact with Plaintiffs and the Class;

j. Whether Defendant breached that contract by failing to adequately safeguard Plaintiffs and Class members' Private Information;

k. Whether Defendant was unjustly enriched;

l. Whether Plaintiffs and Class members are entitled to damages as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class members are entitled to restitution as a result of Defendant's wrongful conduct.

106. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class all had information stored in Defendant's system, each having their Private Information exposed and/or accessed by an unauthorized third party.

107. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs are adequate representative of the Class because their interests do not conflict with the interests of the other Class members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex Class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore,

the interests of the Class members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

108. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

109. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

110. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

111. Likewise, issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations and the HIPAA Privacy Rule, and measures recommended by data security experts would have reasonably prevented the Data Breach.

112. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class members' names and addresses affected by the Data Breach. Defendant has already preliminarily identified Class members for the purpose of sending notice of the Data Breach.

VI. CLAIMS

COUNT 1: NEGLIGENCE
(Plaintiffs on behalf of the Class)

113. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

114. Plaintiffs bring this claim individually and on behalf of the Class.

115. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, and control.

116. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

117. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

118. Defendant's duty also arose from the fact that it holds itself out as a trusted provider of financial services, and thereby assumes a duty to reasonably protect consumers' information.

119. Defendant breached the duties owed to Plaintiffs and Class members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiffs and Class members' Private Information, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Private Information;

(b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

(c) failing to design and implement information safeguards to control these risks;

(d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

(e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

(f) failing to detect the breach at the time it began or within a reasonable time thereafter;

(g) failing to follow its own privacy policies and practices published to its consumers; and

(h) failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive Private Information.

120. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their Private Information would not have been compromised.

121. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now

have prime opportunities to commit identity theft, medical fraud, and other types of attacks on Plaintiffs and Class members.

122. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT 2: NEGLIGENCE PER SE
(Plaintiffs on behalf of the Class)

123. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

124. Plaintiffs bring this claim individually and on behalf of the Class.

125. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

126. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving Private Information of its consumers.

127. Plaintiffs and Class members are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

128. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

129. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

130. As a direct and proximate result of Defendant's negligence, Plaintiffs have been injured as described herein, and is entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT 3: BREACH OF FIDUCIARY DUTY
(Plaintiffs on behalf of the Class)

131. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

132. Plaintiffs and Class members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

133. As a provider of healthcare services and a recipient of consumers' Private Information, Defendant has a fiduciary relationship to its consumers, including Plaintiffs and Class members.

134. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable Private Information related to Plaintiffs and the Class. Plaintiffs and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

135. Defendant owed a fiduciary duty under common law to Plaintiffs and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

136. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiffs' and Class members' Private Information.

137. Defendant's consumers, including Plaintiffs and Class members, have a privacy interest in personal financial matters, and Defendant had a fiduciary duty not to such personal data of its consumers.

138. As a result of the parties' relationship, Defendant had possession and knowledge of confidential Private Information of Plaintiffs and Class members, information not generally known.

139. Plaintiffs and Class members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

140. Defendant breached its fiduciary duties owed to Plaintiffs and Class members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the Data Breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its consumers; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive Private Information.

141. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiffs and Class members, their Private Information would not have been compromised.

142. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs.

143. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT 4: BREACH OF CONFIDENCE
(Plaintiffs on behalf of the Class)

144. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

145. Plaintiffs and Class members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

146. As a provider of healthcare services and a recipient of consumers' Private Information, Defendant has a fiduciary relationship to its consumers, including Plaintiffs and Class members.

147. Plaintiffs provided Defendant with his personal and confidential Private Information under both the express and/or implied agreement of Defendant to limit the use and disclosure of such Private Information.

148. Defendant owed a duty to Plaintiffs to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its

possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

149. As a result of the parties' relationship, Defendant had possession and knowledge of confidential Private Information of Plaintiffs.

150. Plaintiffs' Private Information is not generally known to the public and is confidential by nature.

151. Plaintiffs did not consent to nor authorize Defendant to release or disclose his Private Information to an unknown criminal actor.

152. Defendant breached the duties of confidence it owed to Plaintiffs when Plaintiffs' Private Information was disclosed to unknown criminal hackers.

153. Defendant breached its duties of confidence by failing to safeguard Plaintiffs' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its consumers; (h) storing Private Information in an unencrypted and

vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs' Private Information to a criminal third party.

154. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiffs, their privacy, confidences, and Private Information would not have been compromised.

155. As a direct and proximate result of Defendant's breach of Plaintiffs' confidences, Plaintiffs have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' data; and

i. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant.

156. Additionally, Defendant received payments from Plaintiffs for services with the understanding that Defendant would uphold its responsibilities to maintain the confidences of Plaintiffs' Private Information.

157. Defendant breached the confidence of Plaintiffs when it made an unauthorized release and disclosure of their Private Information and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiffs' expense.

158. As a direct and proximate result of Defendant's breach of its duty of confidences, Plaintiffs are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT 5: INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(Plaintiffs on behalf of the Class)

159. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

160. Plaintiffs had a reasonable expectation of privacy in the Private Information Defendant mishandled.

161. Defendant's conduct as alleged above intruded upon Plaintiffs and Class members' seclusion under common law.

162. By intentionally failing to keep Plaintiffs' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs and Class members' private affairs in a manner that identifies Plaintiffs and Class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class members.

163. Defendant knew that an ordinary person in Plaintiffs or Class members' position would consider Defendant's intentional actions highly offensive and objectionable.

164. Defendant invaded Plaintiffs and Class members' right to privacy and intruded into Plaintiffs and Class members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

165. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

166. The conduct described above was directed at Plaintiffs and Class members.

167. As a proximate result of such intentional misuse and disclosures, Plaintiffs and Class members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

168. In failing to protect Plaintiffs and Class members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs and Class

members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf themselves and the Class.

169. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT 6: BREACH OF IMPLIED CONTRACT
(Plaintiffs on behalf of the Class)

170. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

171. Plaintiffs bring this claim individually and on behalf of the Class.

172. When Plaintiffs and Class members provided their Private Information to Defendant in exchange for healthcare services, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiffs and Class members' Private Information, comply with statutory and common law duties to protect their Private Information, and to timely notify them in the event of a data breach.

173. Defendant solicited and invited Plaintiffs and Class members to provide their Private Information as part of Defendant's provision of services. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant.

174. When entering implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' Private Information and to timely notify them in the event of a data breach.

175. Defendant's implied promise to safeguard consumers' Private Information is evidenced by, *e.g.*, the representations in Defendant's Notice of Privacy Policy set forth above.

176. Plaintiffs and Class members paid money to Defendant in order to receive services. Plaintiffs and Class members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

177. Plaintiffs and Class members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information as promised or provide timely notice of a data breach.

178. Plaintiffs and Class members fully performed their obligations under their implied contracts with Defendant.

179. Defendant breached its implied contracts with Plaintiffs and Class members by failing to safeguard Plaintiffs and Class members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

180. The losses and damages Plaintiffs and Class members sustained include, but are not limited to:

a. Theft of their Private Information;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent financial and medical charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

181. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT 7: UNJUST ENRICHMENT
(Plaintiffs on behalf of the Class)

182. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

183. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' implied contract claim.

184. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class members.

185. As such, a portion of the payments made by or on behalf of Plaintiffs and Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

186. Plaintiffs and Class members conferred a monetary benefit on Defendant. Specifically, they purchased services from Defendant and/or its agents and in so doing

provided Defendant with their Private Information. In exchange, Plaintiffs and Class members should have received from Defendant the services that were the subject of the transaction and have their Private Information protected with adequate data security.

187. Defendant knew that Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class members for business purposes.

188. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

189. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

190. Defendant failed to secure Plaintiffs and Class members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

191. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

192. If Plaintiffs and Class members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

193. Plaintiffs and Class members have no adequate remedy at law.

194. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their Private Information;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

195. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

196. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that it unjustly

received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class members overpaid for Defendant's services.

COUNT 8: DECLARATORY JUDGMENT
(Plaintiffs on behalf of the Class)

197. Plaintiffs restate and reallege the preceding allegations the paragraphs above as if fully alleged herein.

198. Plaintiffs bring this claim individually and on behalf of the Class.

199. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those described herein, that are tortious and violate the terms of the federal statutes described in this Complaint.

200. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk of further compromises of their Private Information will occur in the future.

201. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' Private Information.

202. Defendant still possesses the Private Information of Plaintiffs and the Class.

203. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

204. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial.

205. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Defendant, Plaintiffs and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

206. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose Private Information would be further compromised.

207. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, prays for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representative and their counsel as Class Counsel;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and

Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiffs on all claims so triable.

Dated: December 30, 2024

Respectfully submitted,

/s/ *Sonal Jain*
Sonal Jain
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: sjain@sirillp.com
E. tbeam@sirillp.com

Marc H. Edelson (NY ID 9179646)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
Tel: (215) 867-2399
E: medelson@edelson-law.com

Attorneys for Plaintiffs and the Putative Class

**Pro Hac Vice to be Filed*